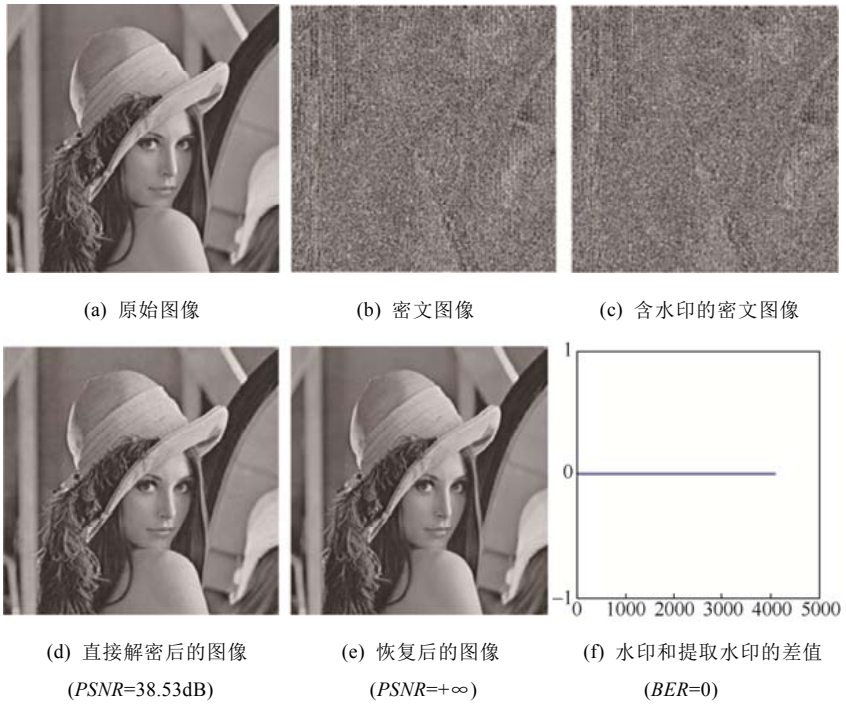
地解决了可能发生的溢出情况.

3 实验结果及分析

实验中首先给出以 Lena 图像作为载体的实验结果来验证本文算法的可行性.本文采用峰值信噪比 PSNR(peak signal to noise ratio)来衡量解密后含水印的图像质量,其值越高,则表示嵌入水印的不可感知性越强,图像的质量越好.假设 I 代表原始图像,I' 代表解密后含水印的图像,(i,j)表示图像像素坐标,则 PSNR 的计算公式为

$$PSNR = 10 \times \lg \frac{h \times w \times 255^2}{\sum_{i=1}^{h}\sum_{j=1}^{w}[I(i,j) - I'(i,j)]^2} \tag{40}$$

其中,h 和 w 代表图像的尺寸,$i \in [1,h]$, $j \in [1,w]$. 另外,本文采用比特误差率 BER(bit error rate)来衡量提取水印的正确性,其值越低,表明提取水印的正确性越高.实验中选取大小为 512×512 的 8 比特的 Lena 灰度图像(如图 8(a)所示)作为测试图像,嵌入的水印是一段 4 096 比特的伪随机序列,采用 Paillier 加密系统的参数设置为 p=61, q=67,其可加密的明文的上限值 $N=p\cdot q$=4087.具体的实验结果如图 8 所示.首先对图 8(a)所示的原始图像进行 8×8 分块并利用公钥(N,g)和密钥 K_s 进行加密得到密文图像(如图 8(b)所示),然后利用嵌入密钥(T=128,G=64)嵌入水印得到含水印的密文图像(如图 8(c)所示).其中,图 8(b)和图 8(c)皆为归一化后的密文图像,目的是显示图像加密后的效果.通过私钥λ对图 8(c)进行解密得到直接解密后的图像(如图 8(d)所示),该图像的 PSNR 为 38.53dB.最后通过嵌入密钥(T=128,G=64)提取嵌入的水印和恢复图像(如图 8(e)所示),该图像的 PSNR 为+∞,表明恢复出来的图像与原始图像完全相同,图 8(f)表明对所有水印比特完成了正确提取.实验结果说明,本文算法实现了加密域中水印的可逆嵌入和提取以及原始图像的恢复.



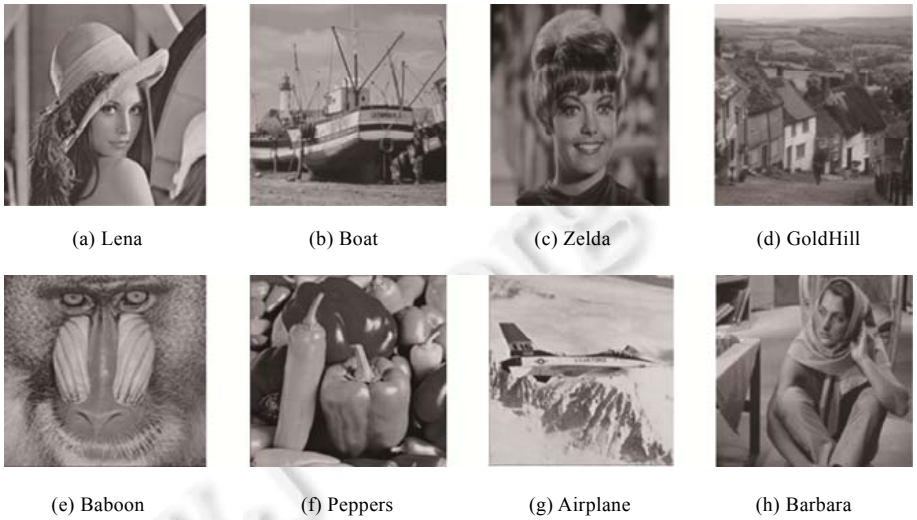
(a) 原始图像 (b) 密文图像 (c) 含水印的密文图像

(d) 直接解密后的图像 (*PSNR*=38.53dB) (e) 恢复后的图像 (*PSNR*=+∞) (f) 水印和提取水印的差值 (*BER*=0)

Fig.8 Watermark embedding and extraction testing results with Lena

图 8 以 Lena 图像为载体的水印嵌入和提取测试

为了更进一步地评估本文算法的性能,实验选取了如图 9 所示的 8 幅大小为 512×512 的 8 比特灰度图像作为载体进行测试.实验中对 8 幅载体图像进行 8×8 分块,嵌入的水印信息为 4 096 比特的伪随机系列.加密域嵌入水印后,密文值的改变相当于其相应的明文值加上了一个大小为嵌入系数 B 的值,因此,B 直接影响到解密后图像的质量.随着 B 的增大,相应的失真就越大,导致 PSNR 降低.经过测试,当 8 幅图像以相同的 B 嵌入水印时,解密后图像的 PSNR 值基本相同,嵌入系数 B 和 PSNR 值的关系如图 10 所示.由图 10 可知,当 B 为 16 时,图像的 PSNR 略大于 30dB,基于不可觉察度的考虑,为了获得较好的图像质量,本文设定最大嵌入系数 B_{max}=16,即 B 的值不能超过 16.



(a) Lena (b) Boat (c) Zelda (d) GoldHill

(e) Baboon (f) Peppers (g) Airplane (h) Barbara

Fig.9 Eight standard example images

图 9 8 幅标准测试图像

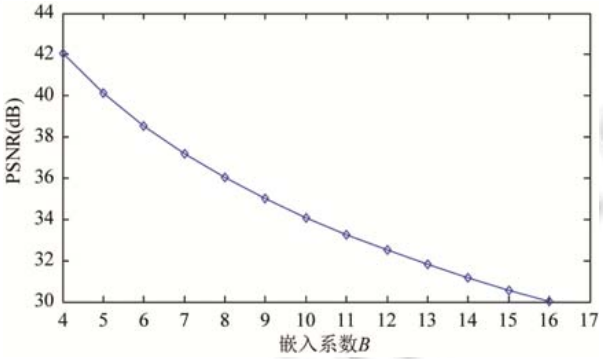


Fig.10 Relationship between embedding strength B and PSNR value

图 10 嵌入强度 B 和 PSNR 值的关系

由图 6 可知,比特 0 区和比特 1 区间隔着大小为 G 的鲁棒区间,G 越大,则鲁棒性越强.但是,G 越大会使嵌入系数 B 随之增大,导致 PSNR 值有所降低.因此,实际中可根据需要调节阈值 G,若需要更强的鲁棒性,可以选择较大的阈值 G;若需要水印图像质量更好,则可选择较小的阈值 G.在 JPEG 压缩鲁棒性实验中,我们采用了 ACDsee 14.0 软件对解密后含水印的图像进行 JPEG 压缩.如图 11 所示,随着压缩质量因子数值的降低(表示压缩强度逐渐增大),提取水印的比特误差率 BER 逐渐升高.在同样的压缩强度下,BER 随着阈值 G 的增大而降低,说明随着阈值 G 的增大,嵌入强度增加,水印对 JPEG 压缩的鲁棒性增强.

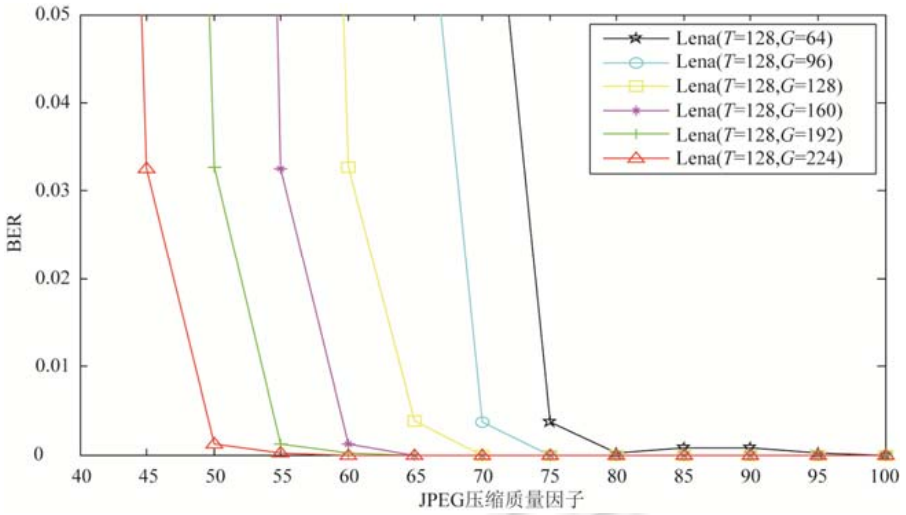


Fig.11 Effection of the value G on the robustness to JPEG compression

图 11 阈值 G 对水印抗 JPEG 压缩的影响

我们采用 ACDsee 14.0 软件对解密后的水印图像进行 JPEG 2000 压缩,采用存活率(surviving bit rate)来衡量水印算法对 JPEG 2000 压缩的鲁棒性.存活率与最大压缩率的关系为:存活率=8/最大压缩率,即存活率越小,其压缩倍数越大,鲁棒性越强.图 12 所示为在不同阈值 G 下能够正确提取水印的最小存活率,即在该阈值下,若存活率高于对应的存活率,即当压缩率更低时,能够完全正确地提取水印.由图 12 可知,随着阈值 G 的增大,最小存活率减小,即水印对抗 JPEG 2000 压缩的鲁棒性增强.

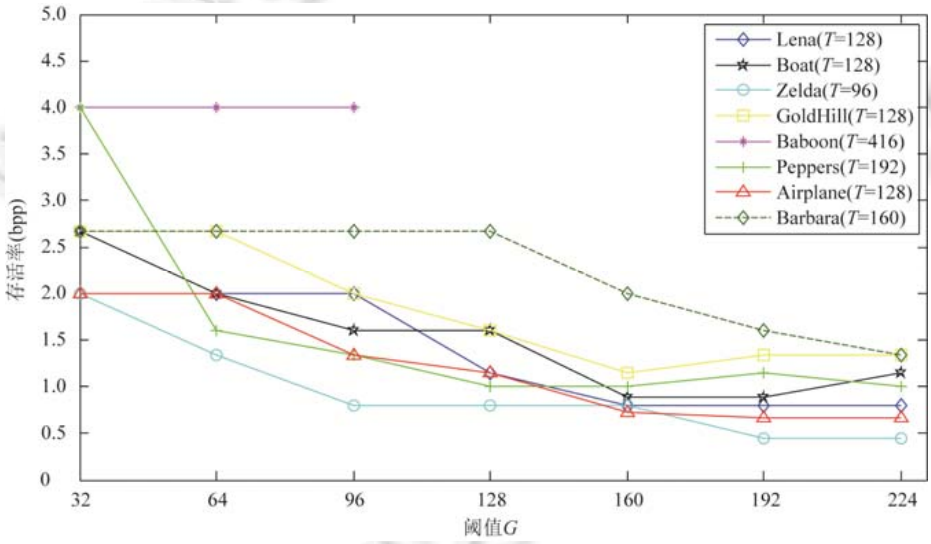


Fig.12 Effection of the value G on the robustness to JPEG 2000 compression

图 12 阈值 G 对水印抗 JPEG 2000 压缩的影响

为了测试本文算法对其他图像处理操作的鲁棒性,本文采用 MATLAB 软件来对水印图像添加高斯噪声和椒盐噪声.表 1 给出了 8 幅测试图像在设定的参数下,嵌入 4 096 比特水印后的解密图像在受到不同图像处理操作后提取水印的比特误差率(BER)(%).嵌入系数 B 设定为 16.从表 1 可以看出,对于质量因子为 25 的 JPEG 压缩,除了 Baboon 图像外,BER 均小于 1%;对于存活率为 0.67bpp 的 JPEG 2000 压缩,除了 Baboon 和 Barbara 图像

外,BER 均小于 1%;对于方差为 0.005 的高斯噪声,除了 Baboon 图像外,BER 均约为 5%;对于方差为 0.01 的椒盐噪声,除了 Baboon 图像外,BER 均小于 5%.与其他测试图像相比,水印以 Baboon 图像为载体性能较差的主要原因是 Baboon 图像的纹理比较复杂,8×8 分块后的 d_{max}=388,需要设定 T=416,即使设定 G=0 都会使嵌入系数 B=13,因此图像的失真较大.在本文设定的最大嵌入系数 B_{max}=16 条件下,G 最大只能取为 96,因此鲁棒性较差.由此可知,本文算法对于比较平滑的图像有较好的性能.

Table 1 Robustness of the proposed method against several image processing operations

表 1 本文水印算法在几种常见图像处理操作下的鲁棒性

测试图像	T	G	PSNR(dB)	JPEG 压缩 (质量因子 25)	JPEG 2000 压缩 (存活率 0.67bbp)	高斯噪声 (方差 0.005)	椒盐噪声 (方差 0.01)
Lena	128	384	30.01	0.10	0	4.93	2.61
Boat	128	384	30.01	0.02	0.02	4.96	2.83
Zelda	96	416	30.01	0.02	0	5.79	3.32
Goldhill	128	384	30.01	0.10	0.05	4.40	2.73
Baboon	416	96	30.01	2.61	48.19	9.25	6.52
Peppers	192	320	30.01	0.29	0.05	4.81	2.71
Airplane	128	384	30.01	0.024	0	5.27	2.83
Barbara	160	352	30.01	0.34	8.45	4.98	2.32

由于每个密文分块都可以嵌入 1 比特水印,所以图像进行分块的尺寸越小,则嵌入容量越大.对于大小为 $h\times w$ 的图像并且分块大小为 $m\times n$ 的最大嵌入容量为$[h/w]\times[w/n]$.其中,函数$\lfloor\cdot\rfloor$为向下取整.但是,通常进行小尺寸分块的嵌入系数 B 会比较大,导致 PSNR 降低.以 Lena 图像为例,当分块尺寸为 4×4 时,它的 d_{max} 为 120,这就意味着:

$$B=\left\lceil\frac{(T+G)\times 2}{m\times n}\right\rceil\geqslant\left\lceil\frac{(128+G)\times 2}{4\times 4}\right\rceil\geqslant 16 \tag{41}$$

设 T 为 128,只有当 G 取 0 时,B=16 才能满足本文设定的 B_{max}=16.为了衡量嵌入容量和图像失真以及鲁棒性的关系,给出 Lena 图像以不同分块尺寸嵌入最大嵌入容量的性能,见表 2.在不超出最大嵌入系数 B_{max}=16 的情况下,除分块尺寸为 4×4 在 JPEG 压缩因子为 100 时提取水印 BER=4.52%、存活率为 4 时提取水印 BER=3.89%,其他分块尺寸下的 JPEG 压缩因子和存活率都是在给定参数下能够正确地提取水印的最小 JPEG 压缩因子和存活率,并且 G 是能正确提取水印的最小阈值.由表 2 可知,若分块尺寸越大,则最大嵌入容量越小,并且图像的失真越小,鲁棒性越强.经过实验测试,其结果表明,8×8 分块在嵌入容量、图像失真和鲁棒性之间有较好的平衡性.

Table 2 The performance of Lena image in different block sizes

表 2 Lena 图像不同分块尺寸的性能

分块尺寸	嵌入容量(bit)	T	G	B	PSNR(dB)	JPEG 压缩因子	存活率(bpp)
4×4	16 384	128	0	16	30.07	100	4
4×8	8 192	128	16	9	35.03	100	4
8×4	8 192	128	16	9	35.03	100	4
8×8	4 096	128	32	5	40.12	98	2.66
8×16	2 048	256	64	5	40.15	93	2
16×8	2 048	256	64	5	40.15	93	2.66
16×16	1 024	256	128	3	44.62	93	2

目前,在文献中尚未有有效的加密域图像鲁棒可逆水印算法的报道,因此无法将本文提出的同态加密域图像鲁棒可逆水印算法与前人的研究结果进行公平对比.为了进一步说明本文算法的鲁棒性,我们与前期具有代表性的一种明文域图像鲁棒可逆水印算法[10]进行了性能比较.测试中,使用相同的载体进行 8×8 分块嵌入相同的水印容量,本文算法与文献[10]中 Ni 算法的鲁棒性比较见表 3.由表 3 可知,除了 Baboon 图像以外,本文算法的图像质量和鲁棒性都优于文献[10].值得一提的是,本文算法是在加密域中嵌入水印,可以更好地在云端保护用户的数据隐私,相比文献[10]以及其他在明文域嵌入鲁棒可逆水印的方案,本文算法更加适用于当下大数据背景下的云计算安全领域.

Table 3 Performance comparison of the proposed method against the Ni's method in Ref.[10]
表 3 与文献[10]中 Ni 算法的鲁棒性能比较

测试图像	文献[10]中 Ni 算法			本文算法				
	PSNR(dB)	嵌入容量(bit)	存活率(bpp)	*T*	*G*	PSNR(dB)	嵌入容量(bit)	存活率(bpp)
Lena	40.20	792	0.80	128	128	43.27	792	0.66
Boat	40.50	560	1.00	128	160	43.54	560	0.61
Baboon	38.70	585	1.60	416	96	38.34	585	2.00

4 结 论

加密域鲁棒可逆水印技术通过加密手段来保护数据在云端的隐私,通过可逆水印来实现对敏感载体的完整性认证并通过鲁棒水印来进行保护数据在解密后的版权.通过结合 Paillier 加密系统、构造统计量和直方图平移技术,本文提出了一种新的同态加密域图像鲁棒可逆水印算法.为了保护数据在云端的隐私并允许对密文数据进行算术操作,数据在上传云端之前进行同态加密.为了能在云端的加密数据中嵌入水印,对图像采用了分块加密和在加密域中构造分块统计量,并结合 Paillier 加密系统的同态特性来实现基于统计量直方图平移的水印嵌入.算法的关键在于密文分块统计量的构造、模乘法逆元 MMI 方法的运用、利用同态特性构建密文映射表和嵌入水印,使得在加密域中可以获得统计量直方图进行水印嵌入.

在本文中,我们对水印算法在加密域和明文域的提取和图像的恢复进行了详细分析,并对可能出现的溢出情况给出了处理方案.最后在实验部分,我们选择一些标准的例子图像来测试算法的可逆性和鲁棒性.实验结果表明:(1) 水印算法的嵌入失真较小,具有良好的保真性;(2) 水印算法是可逆的,在未受到攻击的情况下水印能分别在加密域和明文域提取并且原始密文图像或原始明文图像能够无损恢复;(3) 水印具有良好的鲁棒性,解密后的含水印图像在经受一定的图像处理操作下仍能正确地提取水印.在云计算大数据背景下,由于同态加密域鲁棒可逆水印技术在隐私保护和数据安全上的潜在应用前景,本文算法具有很好的理论研究意义和实用价值.

References:

[1] Honsinger CW, Jones P, Rabbani M, Stoffel JC. Lossless recovery of an original image containing embedded data. Int'l Cl: G06K 9/00 US 6278791 B1, 2001-08-21.

[2] Feng JB, Lin IC, Tsai CS, Chu YP. Reversible watermarking: current status and key issues. Int'l Journal of Network Security, 2006,2(3):161–171.

[3] Celik MU, Sharma G, Tekalp AM, Saber E. Lossless generalized-LSB data embedding. IEEE Trans. on Image Processing, 2005, 14(2):253–266. [doi: 10.1109/TIP.2004.840686]

[4] Tian J. Reversible data embedding using a difference expansion. IEEE Trans. on Circuits and Systems for Video Technology, 2003, 13(8):890–896. [doi: 10.1109/TCSVT.2003.815962]

[5] Ni ZC, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Trans. on Circuits and Systems for Video Technology, 2006,16(3): 354–362. [doi: 10.1109/TCSVT.2006.869964]

[6] Li XL, Yang B, Zeng TY. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. IEEE Trans. on Image Processing, 2011,20(12):3524–3533. [doi: 10.1109/TIP.2011.2150233]

[7] Vleeschouwer CD, Delaigle JE, Macq B. Circular interpretation of histogram for reversible watermarking. In: Proc. of the IEEE Workshop of Multimedia Signal Process. 2001. 345–350. [doi: 10.1109/MMSP.2001.962758]

[8] Vleeschouwer CD, Delaigle JE, Macq B. Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans. on Multimedia, 2003,5(1):97–105. [doi: 10.1109/TMM.2003.809729]

[9] Zou D, Shi YQ, Ni Z, Su W. A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. IEEE Trans. on Circuits and Systems for Video Technology, 2006,16(10):1294–1300. [doi: 10.1109/TCSVT.2006.881857]

[10] Ni Z, Shi YQ, Ansari N, Su W, Sun Q, Lin X. Robust lossless image data hiding designed for semi-fragile image authentication. IEEE Trans. on Circuits and Systems for Video Technology, 2008,18(4):890–896. [doi: 10.1109/TCSVT.2008.918761]

[11] Zeng XT, Ping LD, Pan XZ. A lossless robust data hiding scheme. Pattern Recognition, 2010,43(4):1656–1667. [doi: 10.1016/j.patcog.2009.09.016]

[12] An L, Gao X, Li X, Tao D, Deng C, Li J. Robust reversible watermarking via clustering and enhanced pixel-wise masking. IEEE Trans. on Image Processing, 2012,21(8):3598–3611. [doi: 10.1109/TIP.2012.2191564]

[13] Thabit R, Khoo BE. Capacity improved robust lossless image watermarking. IET Image Processing, 2014,8(11):662–670. [doi: 10.1049/iet-ipr.2013.0862]

[14] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1):71–83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/ SP.J.1001.2011.03958]

[15] Zhang XP. Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 2011,18(4):255–258. [doi: 10.1109/LSP.2011.2114651]

[16] Zhang XP. Separable reversible data hiding in encrypted image. IEEE Trans. on Information Forensics and Security, 2012,7(2):826–832. [doi: 10.1109/TIFS.2011.2176120]

[17] Chen YC, Shiu CW, Horng G. Encrypted signal-based reversible data hiding with public key cryptosystem. Journal of Visual Communication and Image Representation, 2014,25:1164–1170. [doi: 10.1016/j.jvcir.2014.04.003]

[18] Zhang XP, Long J, Wang Z, Cheng H. Lossless and reversible data hiding in encrypted images with public key cryptography. IEEE Trans. on Circuits and Systems for Video Technology, 2016,26(9):1622–1631. [doi: 10.1109/TCSVT.2015.2433194]

[19] Xiang SJ, Luo XR, Shi SX. A novel reversible image watermarking algorithm in homomorphic encrypted domain. Chinese Journal of Computers, 2016,39(3):571–581 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2016.00571]

[20] Xiang SJ, Luo XR. Reversible data hiding in encrypted image based on homomorphic public key cryptosystem. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1592–1601 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5007.htm [doi: 10.13328/j.cnki.jos.005007]

[21] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptographic Techniques Prague. 1999. 233–238. [doi: 10.1007/3-540-48910-X_16]

[22] Zheng PJ, Huang JW. Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. IEEE Trans. on Image Processing, 2013,22(6):2455–2468. [doi: 10.1109/TIP.2013.2253474]

[23] Donald K. The Art of Computer Programming, Volume 2. 3rd ed., Addison-Wesley, 1997. 325–515.

[24] Xiang SJ, Yang L, Wang Y. Robust and reversible audio watermarking by modifying statistical features in time domain. Advances in Multimedia, 2017,2017(3):1–10. [doi: 10.1155/2017/8492672]

附中文参考文献:

[14] 冯登国,张敏,张研,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[19] 项世军,罗欣荣,石书协.一种同态加密域图像可逆水印算法.计算机学报,2016,39(3):571−581. [doi: 10.11897/SP.J.1016.2016.00571]

[20] 项世军,罗欣荣.基于同态公钥加密系统的图像可逆信息隐藏算法.软件学报,2016,27(6):1592−1601. http://www.jos.org.cn/1000-9825/5007.htm [doi: 10.13328/j.cnki.jos.005007]

项世军(1974－),男,贵州普定人,博士,教授, CCF 高级会员,主要研究领域为信息隐藏,加密域信号处理.

杨乐(1993－),男,硕士,主要研究领域为多媒体信息安全,加密域信号处理.